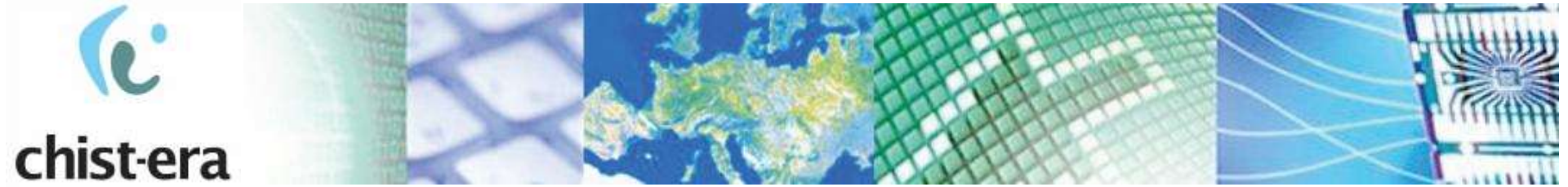


CHIST-ERA Projects Seminar
Day 2, Cross Topics
Resilient Trustworthy Cyber-Physical Systems (RTCPS)

Speaker

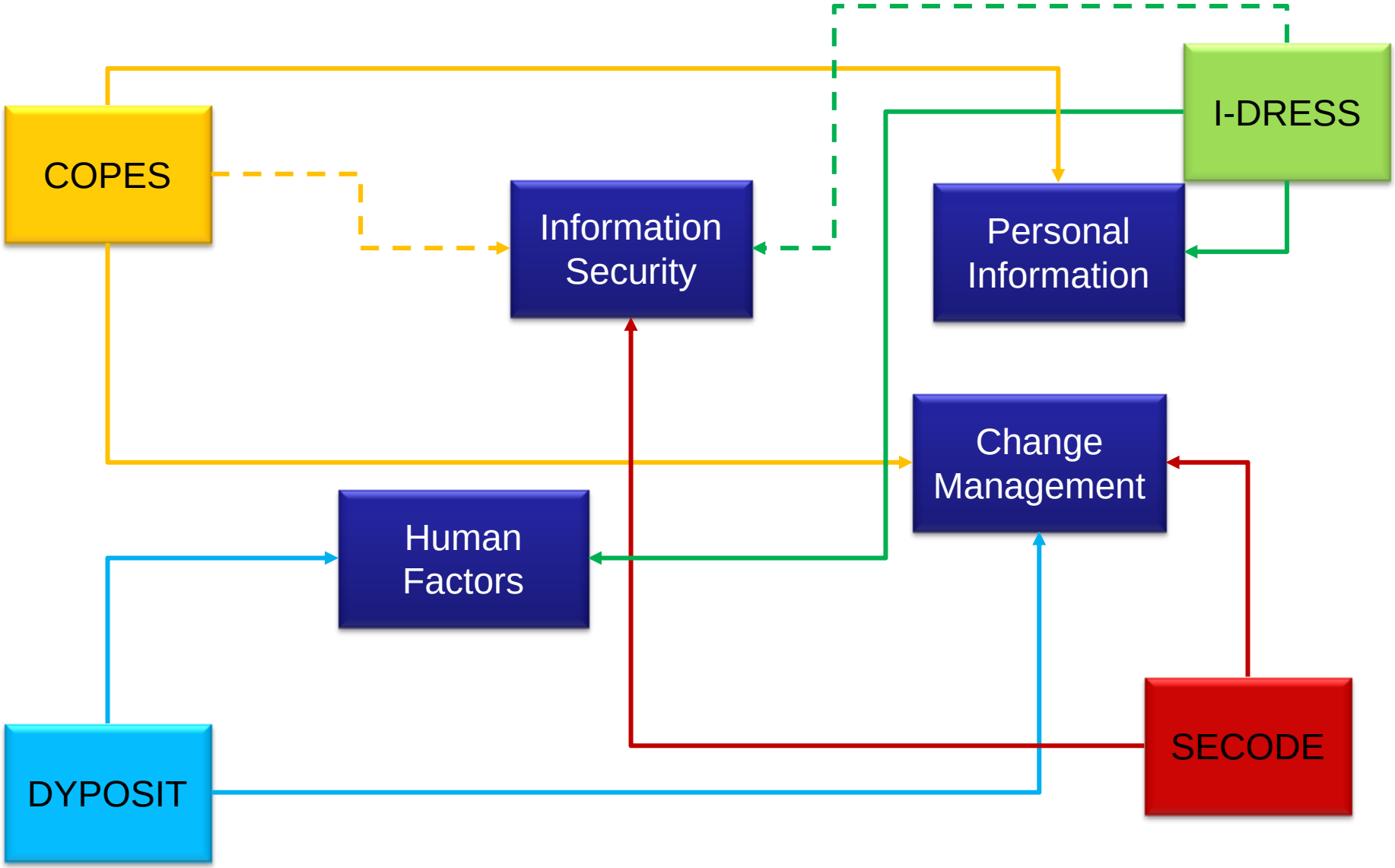
Tobias Oechtering

(KTH, Sweden)

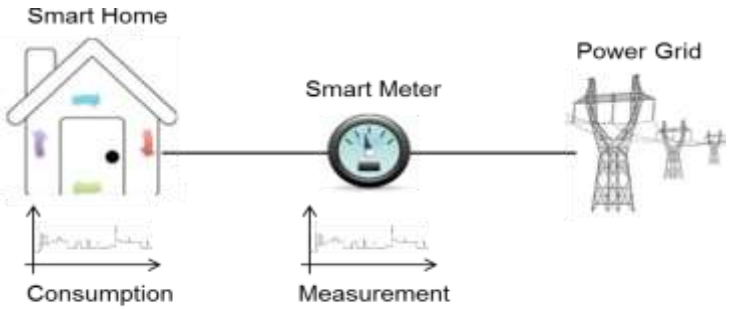
Bern, April 29th, 2016

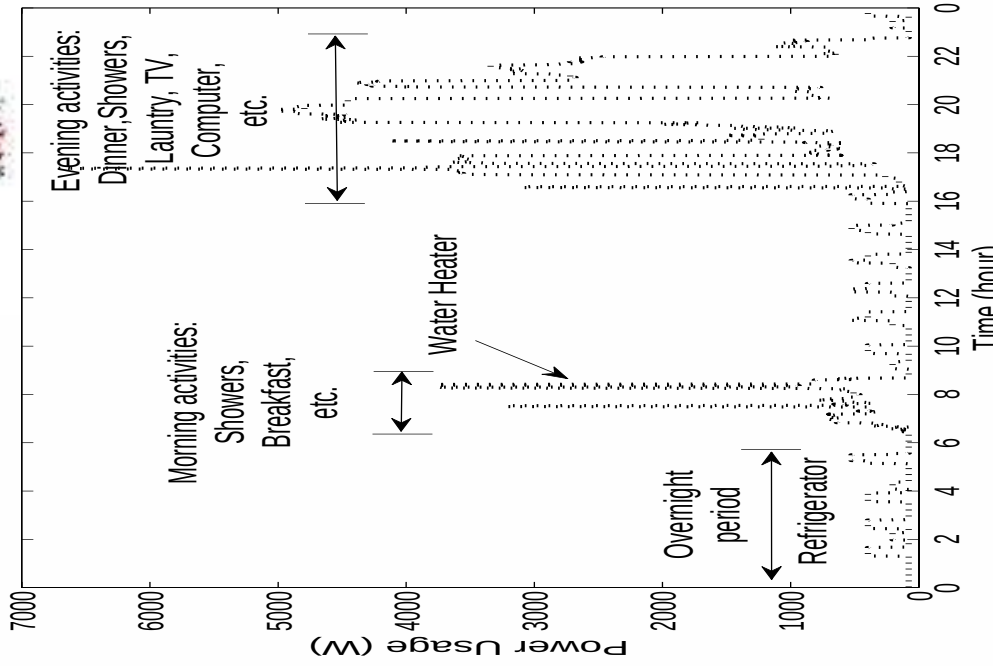
FUNDING OPPORTUNITIES from the FUTURE & EMERGING TECHNOLOGIES scheme

Projects of the Resilient Trustworthy Cyber-Physical Systems (RTCPS)



Smart Meter Privacy Problem



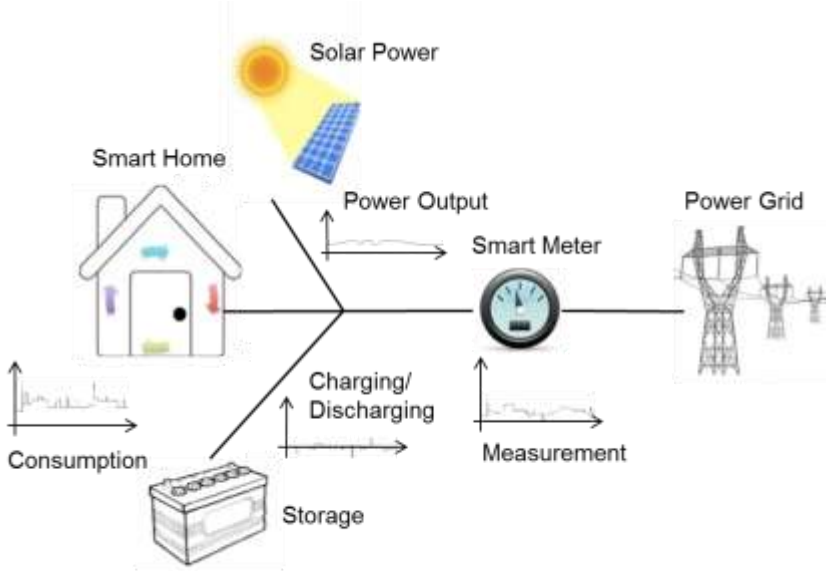


Privacy is

- relevant for **technology adoption**
- **strongly protected** by EU data protection reform
- a potential **show-stopper** (smart grid potentials)

COnsumer-centric Privacy in smart Energy gridS (COPES)

Energy consumption profile reveals sensitive consumer behavior which needs to be protected!



COPES approach: Manipulate actual energy prosumption profile!

COPES core objective

Design of innovative privacy enhancing technologies that

i. allow utility providers to monitor and control the grid, and

ii. assure prosumers' privacy.

KTH VETENSKAP OCH KONST

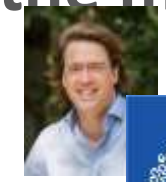
Imperial College London

ETH

Inria

COPES challenges

- **What is the right privacy measure and the most efficient privacy enhancing method?**
  - ✓ Privacy based on statistical inference
  - ✓ Privacy based on information theory
  - ✓ Privacy based on computer science




- **What is the impact on the power system?**
  - ✓ Impact on smart grid control applications
  - ✓ Impact on monitoring and operation

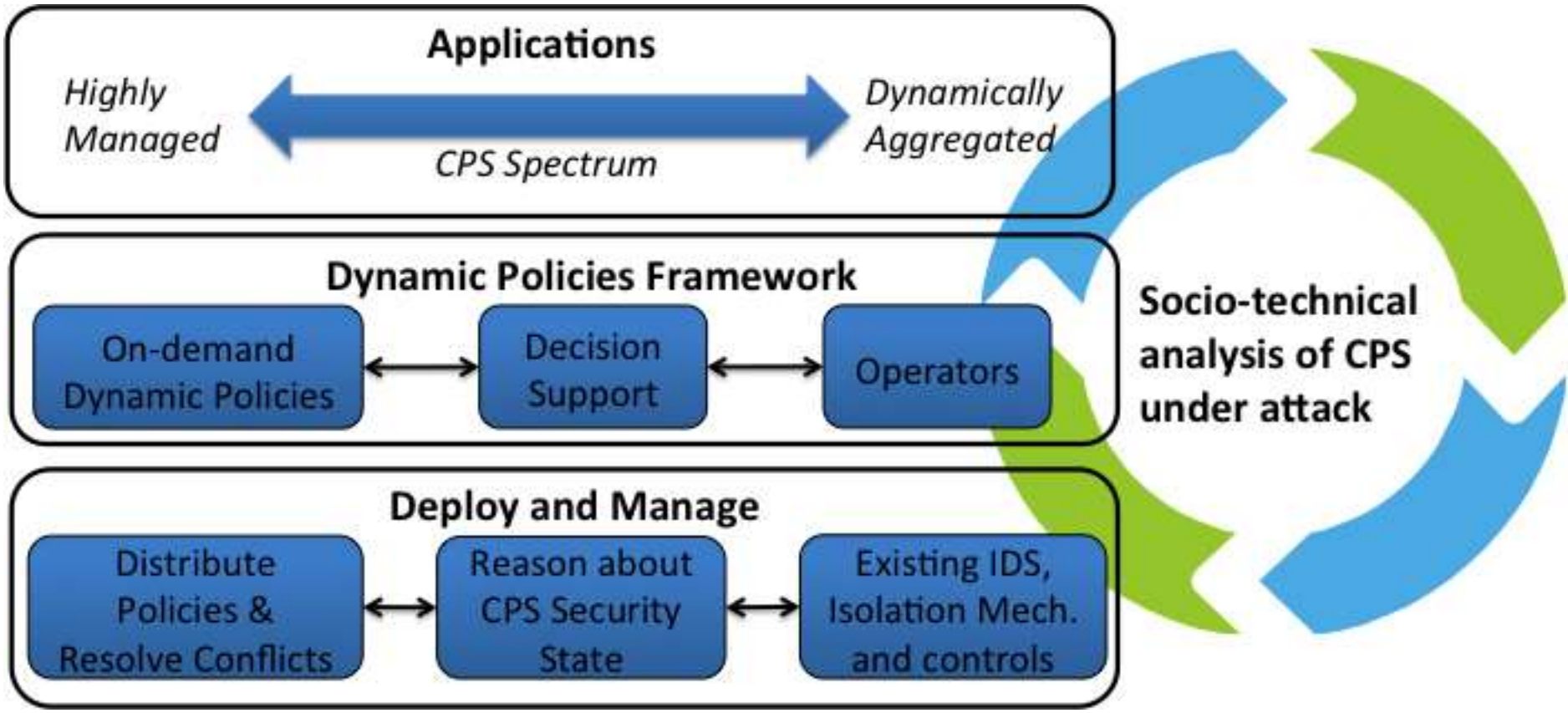

Cross-disciplinarity is necessary for a breakthrough!

DYPOSIT: The Problem

Resilience of large, shared cyber-physical infrastructures under attack

DYPOSIT: Approach

Security policies as living, evolving, objects that play a central role in reasoning about the security state of such a CPS and responding to unfolding attacks.



DYPOSIT: Challenges

- Dynamic security policy formulation, adaptation and enforcement in a volatile, multi-stakeholder environment
- Humans not just part of the problem but part of the solution
- Real-world constraints of shared CPS infrastructures under attack

Actively help users in dressing

- **AIM: to provide PROACTIVE dressing assistance to**
  - ✓ Users with physical or cognitive impairments
  - ✓ high-risk healthcare workers

Safely adapt robot behaviour to changing user needs and preferences, preserving task efficiency

I-DRESS

- **We will develop interaction algorithms to safely interact with users and adapt to unforeseen situations**
- **Scenarios – demos:**
  - ✓ Putting on / taking off a shoe (1 arm task)
  - ✓ Putting on / taking off a medical gown or a coat (2 arms)
- **Platforms:**
  - ✓ WAM arms – IRI, BRL
  - ✓ Baxter robot – IDIAP, BRL

I-DRESS Challenges

- **Human-Robot interaction (HRI):**
  - ✓ Multimodal interaction
  - ✓ Estimation of user preferences, intentions
- **Hazard analysis - safety**
  - ✓ Environment, user reliability, ergonomics
- **Physical and cognitive behaviour**
  - ✓ Learning for safe close interaction
  - ✓ Adaptative robotic behaviour

Institut de Robòtica i Informàtica Industrial — cloth and user recognition, multi-modal HRI and system integration

University of the West of England, Bristol — robot safety, human factors and interface design

idiap Research Institute — robot learning

chist-era

Connected Objects Security Problems

- **Sensitive to cyber attacks**
  - ✓ Perpetrated via the network or by USB keys
  - ✓ Software, taking advantage of weaknesses/bugs
- **Sensitive to physical attacks**
  - ✓ The adversary has access to the objects
  - ✓ and can perform:
    - **Side-channel attacks or probing attacks (passive)**
    - **Fault Injection attacks (active)**

What protections are efficient against both attack types? Can they be **provable**?

SECODE GOALS

Secure Codes to thwart Cyber-physical Attacks

- To specify and design error correction codes for IoT security

Use of codes → **Provide provable security properties**

Attack	Cyber	Physical
Passive	**Randomization** (ASLR, DIFT)	**Randomization** (masking, shuffling, blinding)
Active	**Detection** (canaries, CFI), tolerance (ASLR, code encryption)	**Detection** (redundancy in time, space information), tolerance

SECODE challenges

- **Physical attacks:**
  - ✓ Masking and Detection Multivariate secure with Codes.
  - ✓ Porting to Table-based countermeasures.
- **Cyber-physical attacks**
  - ✓ Modified LLVM embedding protections based on codes.
  - ✓ Protected cryptoprocessor with codes for masking and fault detection.
  - ✓ Demonstrator in FPGA and open source CPU
- **Code specifications:**
  - ✓ Methods to Design "Linear Complementary Dual" LCD codes which are robust against Cyberphysical attacks:
    - **which are “Generalized Quasi Cyclic” (GQC).**
    - **Or defined by an algebraic curve)**
    - **Or others ?**

What does the future hold?

Estimated 50bn connected devices!

chist-era

And not just devices!

Estimated 35 zeta-bytes (35×10^{21}) of digital records!

How do we achieve trustworthy system designs?

What can CHIST-ERA do?

"The journey has just begun"

Questions

Questions ?